GIRARD GIBBS LLP
Eric H. Gibbs – Bar No. 178658
ehg@classlawgroup.com
Amy Zeman – Bar No. 273100
amz@classlawgroup.com
David M. Berger – Bar No. 277526
dmb@classlawgroup.com
Adam E. Polk – Bar No. 273000
aep@girardgibbs.com
Aaron Blumenthal – Bar No. 310605
ab@classlawgroup.com
505 14th Street, Ste. 1110
Oakland, CA 94612
Telephone: 510-350-9700
Facsimile: 510-350-9701

Attorneys for Plaintiff Richard Spicer

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

Richard Spicer, on behalf of himself and all others similarly situated,

Plaintiff,

v.

Equifax Inc. and TrustedID Inc.,

Defendants.

Case No. 17-cv-05228

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Introduction

1. Equifax is a massive data conglomerate, one of the three largest credit reporting agencies in the United States, a credit monitoring company, and a data broker. Its 2017 Annual Report begins with the statement: "We live in a world built on data: it is everywhere, continually growing in power, value and influence." To exploit the value of data, Equifax stockpiles sensitive and personal information about hundreds of millions of consumers. It acknowledges that it must "safeguard[] the data entrusted to us by our customers and consumers" and tells its shareholders that "everything Equifax does revolves around trust."

2. Equifax violated that trust. On September 7, 2017, Equifax announced that hackers had illicitly accessed its computer systems that warehoused data on approximately half of the U.S. population. The hackers used a "U.S. website application vulnerability" to gain access to Equifax's systems, and remained undetected for approximately two-and-a-half months. During that time, they compromised the personal information of approximately 143 million Americans. The compromised data includes names, birth dates, and Social Security numbers. Equifax also allowed the hackers to steal driver's license numbers, credit card information, and other credit history details about hundreds of thousands of consumers. Equifax's statements following the breach indicate that it failed to adopt reasonable security measures relating to perimeter security, application patching, and network segmentation, adequate to ensure that consumers' information was safe inside its computer network. This was not the first time that hackers have exploited Equifax's sub-par cybersecurity controls. Equifax data has been taken in at least four previous data breaches.

3. Equifax knew about the massive 2017 data breach for several weeks before announcing it. When Equifax finally disclosed the incident, it directed consumers to visit the Equifax breach notification website and sign up for a free year of credit monitoring services through a company called TrustedID.

4. Equifax's breach website said that if consumers entered their last name and the last six digits of their Social Security number, the website would tell them whether their information

had been taken in the breach. Equifax also stated that it would provide a free year of TrustedID credit monitoring even to consumers who were *not* affected by the breach.

5. Equifax failed to disclose to consumers that it *owned* TrustedID, and its long-term business model turns on baiting consumers into signing up for its services. In other words, Equifax sought to turn its failure to protect consumers' sensitive data into a clandestine money-making opportunity.

6. Equifax failed to adequately secure consumers' data from unauthorized access. Then, when it was hacked, Equifax failed to promptly and timely notify consumers that their information had been taken. And finally, Equifax tried to exploit the data breach to boost the market share of its own TrustedID product. Plaintiff seeks appropriate relief for Defendants' wrongdoing.

Parties

7. Plaintiff Richard Spicer is a natural person, who is a resident and citizen of California.

8. Defendant Equifax, Inc. is incorporated in Georgia and headquartered in Atlanta, Georgia.

9. Defendant TrustedID Inc. is incorporated in Delaware and headquartered in Palo Alto, California.

Jurisdiction and Venue

10. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from at least one defendant, there are 100 or more Class members, and the aggregate amount in controversy is greater than $5 million. This Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because the action includes a claim arising under federal law.

11. This Court has personal jurisdiction over Defendants because TrustedID Inc. is at home in this district and the claims for relief relate to Defendants' acts and omissions directed to and occurring within this forum.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1931(b)(3) because the Court has personal jurisdiction over Defendants, a substantial portion of the alleged wrongdoing occurred in this District, and Defendants have sufficient contacts with this District.

13. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims arose in this District.

Intradistrict Assignment

14. Assignment to the San Jose Division is proper because a substantial part of the events and omissions which gave rise to the claims occurred at TrustedID's headquarters in Palo Alto, California.

Factual Allegations

How Equifax Acquires Consumer Credit Information

15. Equifax is one of the "Big Three" credit reporting agencies in the United States, along with Experian and TransUnion.[1] When a consumer fills out a credit card or loan application, their information is sent to Equifax and the other credit bureaus.[2] Consumers don't get to choose which credit bureaus receive their information. The banks and credit card companies decide for them.

16. When consumers apply for their *first* credit card or loan, the credit bureaus receive their application information and open a credit file on them. Consumers are advised from an early age that they need to start "building their credit." One prominent financial advice website says, "Building credit can be tricky. If you don't have a credit history, it's hard to get a loan, a credit card or even an apartment."[3] Getting a FICO score,[4] for example, requires a consumer to have a credit account that is at least six months old, with at least one creditor reporting the consumer's

[1] Dave Roos, *How Credit Reporting Agencies Work*, http://money.howstuffworks.com/personal-finance/debt-management/credit-reporting-agency1.htm.

[2] *Id.*

[3] Erin El Issa & Bev O'Shea, *How to Build Credit*, NerdWallet (Oct. 28, 2016), https://www.nerdwallet.com/blog/finance/how-to-build-credit/.

[4] FICO, which stands for Fair Isaac & Company, is the largest and best known of several companies that provide software for calculating a person's credit score.

payment history to credit bureaus during those six months.[5] FICO scores are used by 90% of top lenders to decide whether to extend credit, and at what interest rate.[6]

17. Because the need for credit is so ubiquitous, Equifax captures vast amounts of personal information about nearly every American adult, and many children. As the U.S. Public Interest Research Group notes, "When a credit bureau such as Equifax loses data, it is much more troubling than when a merchant is hacked. When a credit bureau tasked with acting as a gatekeeper to financial and employment success loses the keys to identity theft, that's very scary. How does one of the three major national credit bureaus lose this data?"[7]

Details Regarding Identity Theft Made Possible by Loss of the Information Here

18. Birthdates and Social Security numbers can be used together to steal tax refunds and government benefits, assume the victim's identity on social media, prevent victims from obtaining housing and needed medical prescriptions, damage and destroy credit, and even commit crimes in victims' names. More than 17 million Americans had their identities stolen in 2014, costing them over $15 billion. The GAO further reports that victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft." U.S. Gov't Accountability Office, GAO-14-34, Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent, at 11 (Dec. 2013), *available at* http://www.gao.gov/assets/660/659572.pdf. In 2014, the IRS paid an estimated $3.1 billion in fraudulent tax refunds. *See* U.S. Gov't Accountability Office, GAO-16-589T, IRS Needs to Further Improve Controls Over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud, at 1–2 (Apr. 12, 2016), *available at* http://www.gao.gov/assets/680/676493.pdf.

19. The ramifications of Defendants' failure to keep highly sensitive consumer information secure are severe. The information Defendants lost is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC, About Identity Theft,

---

[5] *Id.*

[6] FICO, *Mimico*, http://www.myfico.com/crediteducation/credit-score.aspx.

[7] U.S. PIRG., *Equifax Breach Puts Millions at Risk of New ID Theft* (Sept. 7, 2017), http://www.uspirg.org/news/usf/equifax-breach-puts-millions-risk-new-id-theft.

available at http://www.wfm.noaa.gov/workplace/PreventingIdentityTheft_About_Handout_2.pdf.

20. Adding to the damage, the Social Security Administration generally will not assign a replacement Social Security number absent "harassment, abuse, or life endangerment," and will consider doing so only after "you've done all you can to fix the problems resulting from misuse of your Social Security number, and someone is still using your number[.]" Soc. Sec. Admin., Can I Change My Social Security Number? (Oct. 21, 2016), *available at* https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-Social-Security-number; Soc. Sec. Admin., Identity Theft and Your Social Security Number, at 6 (Nov. 2016), *available* at https://www.ssa.gov/pubs/EN-05-10064.pdf. Even a "new number probably won't solve all your problems," the Social Security Administration reports. "This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number," and "credit reporting agencies use the [old] number to identify your credit record." *Id*. at 7.

Equifax's Derelict Data Security Resulted in a Massive Breach of Consumer Data

21. The credit bureaus hold a special position of trust, as Congress acknowledged when enacting the Fair Credit Reporting Act: "public confidence" in "credit reporting" is "essential to the continued function of the banking system," and credit reporting agencies "have assumed a vital role in assembling" consumer credit information and other information on consumers.[8] Congress further emphasized the "need to insure that consumer reporting agencies exercise their *grave responsibilities* with fairness, impartiality, and a respect for the consumer's right to privacy."[9]

22. Equifax did not take these "grave responsibilities" seriously. On September 7, 2017, Equifax announced that it had experienced a data breach in which hackers gained unauthorized access to the data of up to 143 million Americans.[10] The compromised data

[8] 15 U.S.C. § 1681.

[9] *Id*.

[10] Equifax, *Form 8-K*, Securities and Exchange Commission (Sept. 7, 2017), http://goo.gl/QxaZ28.

"primarily includes names, Social Security numbers, [and] birth dates," according to Equifax.[11] Also included were, "in some instances, driver's license numbers," "credit card numbers for 209,000 U.S. consumers," and credit dispute documents "with personal identifying information for approximately 182,000 U.S. consumers."[12]

23. Equifax said, in its press release, that it discovered the hack on July 29, 2017, more than one month before announcing the breach.[13] Equifax said that based on "the company's investigation," the hackers had access to Equifax's internal systems from "mid-May through July 2017,"[14] which means that the hackers went undetected in Equifax's systems for two-and-a-half months.

24. Equifax pronounced that "[t]he company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases."[15] This suggests that Equifax designed and maintained a system in which hackers were able to gain access to the sensitive personal information of approximately 143 million Americans without even penetrating Equifax's so-called "core" systems.

25. Equifax did not properly segment and secure its network, if hackers could access the names, birth dates, and Social Security numbers of 143 million people—about half the U.S. population—without needing access to Equifax's "core."

26. Proper network segmentation is a fundamental principle of cybersecurity, and is included on the NSA's list of top 10 critical security controls.[16]

27. As a paper published by the SANS Institute, a leading cybersecurity think tank, explains, "Network segmentation is a fundamental component of an information security strategy; it reduces the likelihood of a compromise from spreading, increases visibility into network traffic, and is the foundation of building a secure network. Without network segmentation, an attacker

---

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] Center for Internet Security, *CIS Critical Security Controls*, https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf.

inside the network can access everything."[17] Proper segmentation requires setting up zones, where the most sensitive data resides in the innermost zone, and less sensitive data resides in outer zones.[18] The innermost zone, also called the "restricted zone," is supposed to house any of the company's "large repositories of sensitive information."[19]

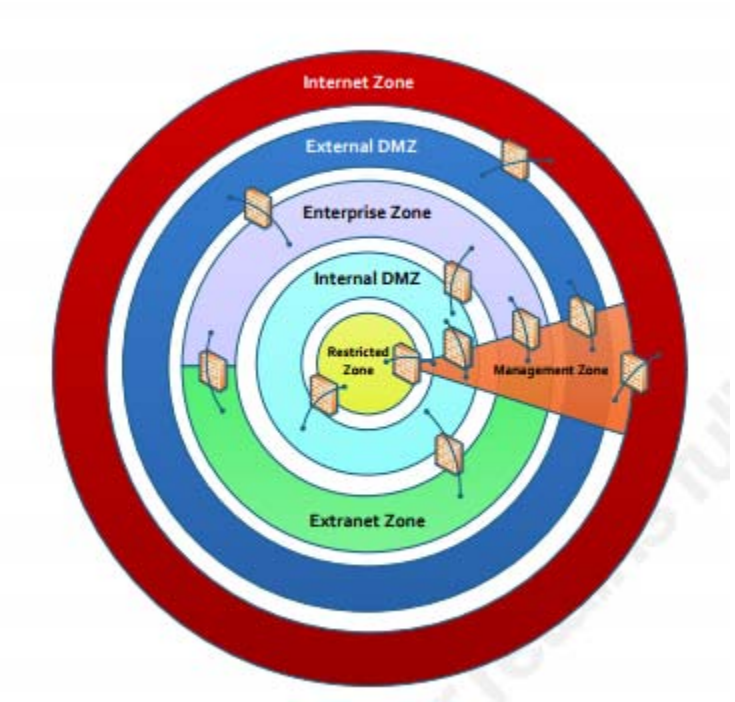

Illustration of Network Segmentation[20]

The inner zone, or "core," is supposed to have far more cybersecurity controls and access restrictions than the other zones or "periphery."

28. Had it implemented proper network segmentation controls, Equifax would not have left the names, birth dates, and Social Security numbers of half of all U.S. citizens vulnerable on the "periphery" of its network.

[17] Luciana Obregon, *Infrastructure Security Architecture for Effective Security Monitoring*, SANS Institute (Dec. 2, 2015), https://www.sans.org/reading-room/whitepapers/bestprac/infrastructure-security-architecture-effective-security-monitoring-36512.

[18] *Id.*

[19] *Id.*

[20] *Id.*

29. Equifax also said, in its press release, that the hackers had exploited a "website application vulnerability" to gain access to the data.[21] As leading cybersecurity writer Brian Krebs notes, the exploitation of an application vulnerability suggests that Equifax was not properly patching and applying security updates to its software.[22]

30. The Australian Signals Directorate, which is Australia's equivalent of the NSA, lists the proper patching of applications as one of the top 4 cybersecurity controls, which could prevent over 85% of all hacking incidents.[23]

31. Equifax also failed to implement adequate administrative controls to protect the sensitive information in its control. As Brian Krebs explains, "It's unclear why Web applications tied to so much sensitive consumer data were left unpatched, but a lack of security leadership at Equifax may have been a contributing factor."[24] Krebs reports that until "very recently," Equifax's role of "vice president of cybersecurity" was vacant.[25] And, according to Equifax, its VP of cybersecurity position "is akin to the role of chief information security officer (CISO)."[26]

32. Doug Drinkwater, a cybersecurity commentator, characterizes "[n]ot employing a chief information security officer" as "foolhardy," and says that in the modern cybersecurity landscape, "it's increasingly clear a CISO is required" because organizations "need someone to build a security infrastructure, [and] to lead security strategy."[27]

33. Equifax's failure to take basic steps to protect its customers' personal information is inexcusable given the company's history of cybersecurity failures and consequent breaches:

---

[21] Equifax, *Form 8-K*, *supra* note 10.

[22] Brian Krebs, *Breach at Equifax May Impact 143M Americans*, KrebsonSecurity (Sept. 7, 2017), https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/.

[23] ASD, *Strategies to Mitigate Targeted Cyber Intrusions* (updated 2017), https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm.

[24] Brian Krebs, *supra* note 22.

[25] *Id*.

[26] *Id*.

[27] Doug Drinkwater, *How and why to hire a CISO*, CSO Online (June 5, 2017), https://www.csoonline.com/article/3199045/security/how-and-why-to-hire-a-ciso.html.

- In March 2014, Equifax reported a breach that occurred between April 2013 and January 2014, in which customer credit reports were compromised.[28]
- In May 2016, Equifax's W-2 Express website suffered a breach that resulted in the compromise of 430,000 names, addresses, Social Security numbers and other personal information.[29]
- In February 2017, Equifax "was forced to confess to a data leak in which credit information of a 'small number' of customers at partner LifeLock had been exposed to another user of the latter's online portal."[30]
- In May 2017, TALX, an Equifax subsidiary that provides online payroll and HR services suffered a breach in which hackers were able to obtain customer W-2 tax data.[31]

Equifax was accordingly aware—prior to this breach—that it presented an attractive target for hackers given the nature and quality of the information on its systems, yet failed to take minimal, industry standard steps to protect it.

Equifax's Deceptive Post-Breach Conduct

34. After the breach occurred, Equifax said that it had "established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted" by the breach and to enable them "to sign up for credit file monitoring and identity theft protection."[32] Equifaxsecurity2017.com tells consumers that Equifax is offering one free year of TrustedID Premier credit monitoring services, which includes "five separate offerings," including: free copies of your Equifax credit report, 3 bureau credit file monitoring, the ability to lock your Equifax credit file, $1 million of identity theft insurance, and Social

[28] Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, Forbes (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#2acb3dc1677c.

[29] *Id*.

[30] *Id*.

[31] Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KrebsonSecurity (May 2017), https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/.

[32] Equifax, *Form 8-K*, *supra* note 10.

Security Number Monitoring—a service that searches the dark web for criminals attempting to sell your Social Security number.[33]

35. The Equifax breach website says that, in addition to people impacted by the data breach, Equifax is also offering one year of free TrustedID Premier services to anyone in the United States, "[r]egardless of whether your information may have been impacted."[34]

36. What Equifax does not disclose (in its press release or on its breach website) is that Equifax bought TrustedID Inc. in 2013.[35] The TrustedID Premier product is an identity monitoring service owned and operated by Equifax.

37. Equifax could have offered identity monitoring services through its own branded service, "Equifax ID Patrol," but chose to instead offer credit monitoring services through its subsidiary, TrustedID.

38. By encouraging all consumers to sign up for TrustedID Premier, Equifax stands to profit significantly from the breach of its own computer network. As Brian Krebs notes, "The fact that the breached entity (Equifax) is offering to sign consumers up for its own identity protection services strikes me as pretty rich. Typically, the way these arrangements work is the credit monitoring is free for a period of time, and then consumers are pitched purchasing additional protection when their free coverage expires."[36]

39. Equifax intends to exploit its own exposure to hacking in precisely this manner. In its 2016 10-K filing with the Securities and Exchange Commission, Equifax noted that many credit monitoring companies were increasingly pursuing a business strategy of "offering free or low-cost direct to consumer credit services (such as credit scores, reports, and monitoring)" and using those free "services as a means to introduce consumers to premium products and services."[37]

---

[33] https://www.equifaxsecurity2017.com/trustedid-premier/.

[34] https://www.equifaxsecurity2017.com/potential-impact/.

[35] San Francisco Business Times, *Equifax buys TrustedID for $30 million* (July 9, 2013), https://www.bizjournals.com/sanfrancisco/morning_call/2013/07/equifax-buys-trustedid-for-30-million.html.

[36] Brian Krebs, *supra* note 22.

[37] Equifax, *Form 10-K*, SEC (2016), at 16, https://goo.gl/ZZFBwA.

40. In a 2014 presentation to investors, Equifax said that one of its "key growth strategies" was to "attack" the $1.6 billion market for non-financial institution products, such as credit monitoring, by utilizing its acquisition of TrustedID as a "foundation."[38] Experian explained that "the US identity protection market [is] estimated to be a US$1.6 billion industry."[39]

41. Much of Equifax's revenue growth has come from its sale of identity protection through TrustedID. Equifax noted in its Annual Statement to investors that it had boosted revenue by 12% in 2013 due to increased sales of "U.S.-based subscription services," sales that were spurred by "the acquisition of TrustedID" in 2013.[40]

42. Equifax's 10-K disclosures show that it earned $402.6 million in revenue from its "Global Consumer Solutions" division in 2016.[41] Equifax explains that "Global Consumer Solutions revenue" is "derived from the sale of credit monitoring and identity theft protection products, which [Equifax] delivers to consumers primarily via the internet."[42]

43. Equifax is attempting to capitalize on the breach of its computer systems by using it as an opportunity to try to carve out a larger share of the $1.6 billion identity protection industry.

44. Equifax also benefits when consumers sign up for TrustedID services by gaining access to a wider trove of data. TrustedID's service monitors all three credit bureaus. To sign up, a consumer must authorize TrustedID to retrieve information about the consumer from the other two credit bureaus (Experian and TransUnion). The information on the credit reports of the bureaus can vary by up to 20%, meaning Equifax can gain access to additional information from

---

[38] Equifax, *Investor Presentation* (Mar. 2014), at 32, https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/events/efxinvestor-conference-presentation-mar-2014.pdf.

[39] Experian, *Definitive Agreement to Acquire CD Identity Corporation* (2016), https://www.experianplc.com/media/news/2016/definitive-agreement-to-acquire-csidentity-corporation/.

[40] Equifax, *2013 Annual Report*, at 17, https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2013-annual-report.pdf.

[41] Equifax, *Form 10-K*, *supra* note 37.

[42] Equifax, *Form 10-Q*, SEC (June 30, 2017), https://goo.gl/vCGMVs.

the other two credit bureaus when consumers grant TrustedID access to their Experian and TransUnion credit files.

45. In addition, Equifax's fraud alert product for its three-bureau monitoring is "made available to consumers by Equifax Information Services LLC."[43] Equifax Information Services LLC is a data broker that sells consumer information. In 2012, Equifax Information Services LLC settled a lawsuit brought by the Federal Trade Commission over its allegedly unlawful selling of consumers' information to third parties who pitched predatory debt relief services to consumers in financial distress.[44]

46. When consumers sign up for TrustedID, they are purportedly agreeing to allow TrustedID to share their personal information with TrustedID's "affiliates"—which include Equifax Information Services LLC.[45]

Plaintiff's Experience

47. Richard Spicer has never had any direct relationship with Equifax. As far as Mr. Spicer is aware, his information resides on Equifax's system only because he has applied for various credit offerings in the United States, and the banks reported his personal information, including his Social Security number, to Equifax. Mr. Spicer learned that he had been a victim of the Equifax data breach when he visited Equifax's breach website and entered his last name and the last six digits of his Social Security number. The breach website notified him that his information had been compromised in the breach, and offered to immediately enroll him in one free year of credit monitoring services with TrustedID.

Class Allegations

48. Pursuant to the Federal Rule of Civil Procedure 23(b)(3), Plaintiff asserts claims on behalf of the following "Class": All persons in the United States whose information was compromised in the data breach announced by Equifax on September 7, 2017. Excluded from the

[43] Equifax, *3-in-1 Monitoring*, http://www.equifax.com/3in1-monitoring-with-4-credit-scores/.

[44] FTC, *FTC Settlements Require Equifax to Forfeit Money Made by Allegedly Improperly Selling Information about Millions of Consumers Who Were Late on Their Mortgages* (Oct. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-settlements-require-equifax-forfeit-money-made-allegedly.

[45] TrustedID, *Privacy Notice*, https://www.trustedid.com/premier/privacy-notice.php.

Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

49. This action has been brought and may properly be maintained as a class action as it satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23(b)(3). Plaintiff seeks to represent an ascertainable Class, as determining inclusion in the class can be accomplished through Equifax's own records.

50. Plaintiff reserves the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses, or modified in any other way.

51. Although the precise number of Class members is unknown and can only be determined through appropriate discovery, Plaintiff believes, and on that basis alleges, that the proposed Class is so numerous that joinder of all members would be impracticable.

52. Questions of law and fact common to the putative Class exist that predominate over questions affecting only individual members, including *inter alia*:

a. Whether Equifax failed to implement adequate data security to protect consumer information in its possession;

b. Whether Equifax breached a duty of care by failing to implement reasonable security measures;

c. Whether Equifax intentionally obscured its relationship with TrustedID to capitalize on the breach to increase its share of the market for identity protection services;

d. Whether Equifax's and TrustedID's conduct constitutes an unfair business practice under California's Unfair Competition Law (UCL);

e. Whether Equifax's and TrustedID's conduct constitutes an unlawful business practice under the UCL for violating the Gramm-Leach-Bliley Act (GLBA);

f. Whether Equifax's and TrustedID's conduct constitutes an unlawful business practice under California's Consumer's Legal Remedies Act;

g. Whether the Class is entitled to compensatory and punitive damages, and in what amount;

h. Whether Equifax and TrustedID should be enjoined from offering their credit monitoring services on the breach website without disclosing their relationship.

53. Plaintiff is a member of the putative Class. The claims asserted by the Plaintiff in this action are typical of the claims of the members of the putative Class, as the claims arise from the same course of conduct by the Defendants and the relief sought is common.

54. Plaintiff will fairly and adequately represent and protect the interests of the members of the putative Class, as his interests are coincident with, not antagonistic to, the other members of the Class.

55. Plaintiff has retained counsel competent and experienced in both consumer protection and class action litigation. Plaintiff's counsel specifically has experience litigating some of the largest and most complex consumer class actions, including numerous consumer class actions in the Northern District of California.

56. Certification of the Class is appropriate pursuant to Fed. R. Civ. P. 23(b)(3) because questions of law or fact common to the respective members of the Class predominate over questions of law or fact affecting only individual members. This predominance makes class litigation superior to any other method available for the fair and efficient adjudication of these claims including consistency of adjudications. Absent a class action it would be highly unlikely that the members of the Class would be able to protect their own interests because the cost of litigation through individual lawsuits might exceed the expected recovery.

57. Certification of the Class is also appropriate pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and/or (c)(4).

58. A class action is a superior method for the adjudication of the controversy in that it will permit a large number of claims to be resolved in a single forum simultaneously, efficiently, and without the unnecessary hardship that would result from the prosecution of numerous individual actions and the duplication of discovery, effort, expense, and the burden of the courts that individual actions would create.

59. The benefits of proceeding as a class action, including providing a method for obtaining redress for claims that would not be practical to pursue individually, outweigh any difficulties that might be argued with regard to the management of the class action.

First Cause of Action
Violation of California's Unfair Competition Law
(against all Defendants)

60. Plaintiff incorporates by reference all allegations, as if fully set forth herein.

61. Defendants violated California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, by engaging in unfair and unlawful business acts and practices.

62. Defendants' conduct constitutes an "unfair" practice, within the meaning of the UCL, because their conduct was unscrupulous and caused substantial harm. This conduct includes: failing to adequately secure consumer data entrusted to them, and attempting to profit from the Equifax data breach by bolstering subscriptions to TrustedID's credit monitoring services, without disclosing that TrustedID is owned by Equifax. Consumers were harmed by having their personal information, including Social Security numbers, made accessible to hackers, subjecting them to an impending risk of identity theft. Social Security numbers are of particular use to identity thieves, and hackers are unlikely to break into a credit bureau without a nefarious intent to utilize stolen information to perpetrate financial fraud. Consumers were also harmed by Equifax and TrustedID's inducing them to sign up for services with TrustedID, and by not disclosing the relationship between the two entities, because consumers thereby provided Equifax access to additional information about themselves that Equifax could sell. These harms outweigh any possible utility of the conduct.

63. The conduct described in the previous paragraph is also "unfair" because it violates the policies of the Fair Credit Reporting Act.

64. Additionally, Defendants' conduct is "unlawful" because it violates the Gramm-Leach-Bliley Act. Under the GLBA, financial institutions, such as Defendants, are required to "develop, implement, and maintain a comprehensive information security program" that contains appropriate "administrative, technical, and physical safeguards" to protect the security of customers' information. Defendants did not adopt administrative and technical safeguards that

would be appropriate given Defendants' size and complexity, the scope and importance of Defendants' credit monitoring activities, and the sensitivity of the customer information that was at risk. Because Defendants failed to adopt appropriate security controls commensurate with the risk, Plaintiff and the Class's information was compromised by hackers.

65. Plaintiff and the Class were injured and lost money or property as a result of Defendants' unfair and unlawful practices because they face imminent risk of identity theft, and lost value of their personal information (which Equifax normally charges a fee to access).

Second Cause of Action
Violation of Credit Repair Organizations Act (CROA)
(against all Defendants)

66. Plaintiff incorporates by reference all allegations, as if fully set forth herein.

67. Defendants are credit repair organizations, within the meaning of 15 U.S.C. § 1679a, because, among other things, they use an instrumentality of interstate commerce (*e.g.*, the internet) or the mail to sell, provide, or perform (or represent that they will sell, provide, or perform) a service in exchange for money or other valuable consideration for the express or implied purpose of advising and assisting consumers concerning their credit record and credit rating.

68. As a credit repair organization, it is unlawful for Defendants to make or use any untrue or misleading representation of its services, or engage—directly or indirectly—in any act, practice, or course of business that constitutes or results in the commission, or an attempt to commit, a fraud or deception on any person in connection with the offer or sale of its services.

69. As previously alleged, Defendants engaged in misleading representations of their services and engaged in a course of conduct that constitutes fraud or deception on consumers in connection with the offer of their services, because Defendants omitted material information on the Equifax breach website in an attempt to make TrustedID credit monitoring and identity protection appear to be a wholly separate service from those offered by Equifax, induce consumers to provide additional information to TrustedID and Equifax, and purport to bind consumers to binding arbitration in exchange for offering credit monitoring, repair, and identity theft protection services.

70. As Defendants have failed to comply with the provisions of CROA, they are liable for the greater of: (1) the amount of any actual damage sustained by such persons as a result of such failure; or (2) any amount paid by Plaintiff and the Class members to Equifax or TrustedID. In addition, as the above conduct was directed at potentially hundreds of millions of persons, was frequent in terms of the nature of such noncompliance, was intentional because Equifax planned to use the breach to bolster TrustedID's user base, and has violated numerous basic provisions of the statute, among other relevant factors, Defendants are also liable under CROA for punitive damages. If this action is certified to proceed as a class action, Plaintiff and the Class members would be entitled to the sum of: (1) the aggregate of the amount which the Court may allow for each named plaintiff; and (2) the aggregate of the amount which the Court may allow for each other class member, without regard to any minimum individual recovery.

71. Plaintiff and the Class seek actual and punitive damages, attorneys' fees, and costs pursuant to 15 U.S.C. § 1679g.

Third Cause of Action
Negligence
(against Equifax)

72. Plaintiff incorporates by reference all allegations, as if fully set forth herein.

73. Equifax required the collection of personal information to perform its services. As evinced by the intent of the Fair Credit Reporting Act, the collection of vast stores of personal information by a credit reporting agency creates a duty on behalf of the agency to safeguard to privacy and integrity of the data.

74. Equifax owed a duty of care to Plaintiff and the Class, whose personal information was entrusted with Equifax. Equifax knew or should have known of the risks inherent in collecting and storing large amounts of personal information, given the sensitivity and scale of the data. Equifax could reasonably foresee that a failure to implement adequate security controls would lead to compromise of the data in a cyber-intrusion. Equifax's duty to exercise reasonable care included, among other things, designing, maintaining, monitoring, and testing its security systems, protocols, and practices to ensure that the information of the Class was adequately secured from unauthorized access.

75. Equifax also owed a duty to disclose the material fact that its data security practices were inadequate to safeguard the personal information of the Class.

76. Equifax also had independent duties under state laws requiring it to reasonably safeguard the personal information of the Class, and promptly notify them about the breach.

77. Equifax had a special relationship with the Class because it was entrusted with their personal information, which provided an independent duty of care. The Class's willingness to entrust Equifax with their Personal Information, or to engage in activities that would result in Equifax obtaining their Personal Information, was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and stored personal information from attack.

78. Equifax's role in collecting, utilizing, and purportedly safeguarding the Class's personal information presents unique circumstances necessitating a reallocation of risk.

79. Equifax breached its duties by, among other things: (a) failing to implement and maintain fair, reasonable, or adequate computer systems and data security practices to safeguard the personal information of the Class; (b) failing to detect the breach in a timely manner; (c) failing to implement proper segmentation and patching of its systems, (d) failing to disclose that its data security practices were inadequate to safeguard the personal information of the Class; and (e) failing to provide adequate and timely notice of the breach.

80. But for Equifax's breach of its duties, the personal information of the Class would not have been accessed by unauthorized individuals, and identity theft could have been prevented.

81. The injury and harm suffered by Plaintiff and proposed class members was the reasonably foreseeable result of Equifax's breach of its duties. Equifax knew or should have known that it was failing to meet its duties and that a breach of its data systems would cause the Class to experience the foreseeable harms associated with the exposure of their personal information.

82. As a result of Equifax's willful conduct in failing to prevent the data breach, Plaintiff and the Class suffered injury, including exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff the Class must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members have

also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' personal information has also diminished the value of the personal information.

83. As a direct and proximate result of Equifax's negligent conduct, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

84. Defendants' conduct was also negligent per se.

85. As alleged above, Equifax was required under the Gramm-Leach-Bliley Act to satisfy certain standards relating to administrative, technical, and physical safeguards, including:

> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

12 U.S.C. § 6801(b).

86. To satisfy its obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

87. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

88. Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.*

89. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failing to implement and maintain fair, reasonable, or adequate computer systems and data security practices to safeguard the personal information of proposed class members; (b) failing to detect the breach in a timely manner; (c) failing to implement proper segmentation and patching of its systems, (d) failing to disclose that its data security practices were inadequate to safeguard the personal information of the Class; and (e) failing to provide adequate and timely notice of the breach.

90. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, its failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the data breach in a timely and adequate manner.

91. Equifax further violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

92. Plaintiff and Class were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class members themselves, would cause damages to the Class.

93. Equifax's failure to comply with the applicable laws and regulations, including the GLBA, constitutes negligence per se.

94. But for Equifax's violation of the applicable laws and regulations, the Class's personal information would not have been accessed by unauthorized individuals.

95. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff and the Class suffered injury, which includes but is not limited to exposure to a

heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and the Class must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff and the Class's personal information has also diminished the value of the personal information.

96. The injuries to Plaintiff and the proposed class members were the proximate and reasonably foreseeable results of Equifax's breaches of the applicable laws and regulations.

97. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

Fourth Cause of Action
Violation of the California Customer Records Act (CRA)
(against Equifax)

98. Plaintiff incorporates by reference all allegations, as if fully set forth herein.

99. California Civil Code requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

100. Equifax owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, about Plaintiff and the Class.

101. Equifax violated Civil Code § 1798.81.5 by failing to implement reasonable measures to protect the personal information of the members of the Class.

102. The data breach described above occurred as a direct and proximate result of Equifax's violations of section 1798.81.5 of the California Civil Code.

103. Additionally, California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose

unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . ."

104. Section 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

105. Equifax is a business that owns or licenses computerized data includes personal information as defined by Cal. Civ. Code § 1798.80 *et seq.*

106. In the alternative, Equifax maintains computerized data that includes personal information that it does not own as defined by Cal. Civ. Code § 1798.80 *et seq.*

107. The personal information (including but not limited to names, birth dates, and Social Security numbers) of the members of the Class includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

108. Because Equifax reasonably believed that the personal information of the members of the Class was acquired by unauthorized persons, it had an obligation to disclose the data breach described above in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

109. By failing to disclose the data breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

110. As a direct and proximate result of Equifax's violations of §§ 1798.81.5 and 1798.82 of the California Civil Code, Plaintiff and the members of the Class suffered the damages described above, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

111. Plaintiff and the Class seek relief under § 1798.84 of the California Civil Code, including, but not limited to, actual damages in an amount to be proven at trial, and injunctive relief.

Fifth Cause of Action
Violation of the California Consumers Legal Remedies Act (CLRA)
(against all Defendants)

112. Plaintiff incorporates by reference all allegations, as if fully set forth herein.

113. The CLRA proscribes "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale of goods or services to any consumer."

114. Defendants are "persons" within the meaning of the CLRA. Cal. Civ. Code § 1761(c).

115. Equifax and TrustedID credit monitoring is a "service" within the meaning of the CLRA. Cal. Civ. Code § 1761(b).

116. Plaintiff and members of the Class are "consumers" within the meaning of the CLRA. Cal. Civ. Code § 1761(d).

117. As alleged herein, Defendants made numerous representations concerning source, sponsorship, characteristics, affiliations, and effects of their credit monitoring services, and failed to disclose the ownership of TrustedID, that TrustedID would result in additional information being aggregated in Equifax's insecure databases, and that the TrustedID Terms of Service included an arbitration provision with a class action waiver. Plaintiffs and the Class members were deceived by Defendants' failures to disclose this information.

118. Defendants' conduct, as described herein, was and is in violation of the CLRA, including the following enumerated provisions:

a. § 1770(a)(1): Passing off goods or services as those of another;

b. § 1770(a)(2) Misrepresenting the source, sponsorship, approval, or certification of goods or services;

c. § 1770(a)(3) Misrepresenting the affiliation, connection, or association with, or certification by, another;

d. § 1770(a)(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that he or she does not have;

e. § 1770(a)(14) Representing that a transaction confers or involves rights, remedies, or obligations that it does not have or involve, or that are prohibited by law;

f. § 1770(a)(19) Inserting an unconscionable provision in the contract.

119. Plaintiff and the Class members have suffered injury in fact and actual damages resulting from Defendants' material omissions and misrepresentations because they lost money, including the value of their personal information and other legal rights, when they provided personal information to Defendants and signed up for the TrustedID service.

120. Defendants knew, should have known, or were reckless in not knowing that TrustedID Premier was and is provided by Equifax and that Plaintiffs' personal information provided to TrustedID would be incorporated into Equifax's inadequately secured computer systems.

121. Defendants had a duty to disclose the relationship between TrustedID and Equifax because Defendants had exclusive knowledge of this prior to encouraging Plaintiff and the Class members to sign up for TrustedID Premier in the wake of the Equifax data breach announcement and because they made partial representations about the quality, affiliation, and sponsorship of TrustedID Premier and the effects of signing up for the service.

122. The facts that Defendants concealed and omitted to Plaintiffs and the Class members are material in that a reasonable consumer would have considered them to be important in deciding whether to sign up for the TrustedID Premier service and whether to hand over their valuable personal information.

123. Had Defendants been truthful and candid about these issues, Plaintiff and the Class members would not have signed up for TrustedID Premier or would have refused to provide additional, valuable personal information to Defendants in the process.

124. This cause of action seeks injunctive relief only at this time, it does not seek damages or other monetary relief. Plaintiff, however, is sending a demand letter to each Defendant via certified mail pursuant to the requirements of the CLRA, Cal. Civ. Code § 1782(a). If Defendants do not correct or otherwise rectify the harm alleged by Plaintiff in his letter or this Complaint within the statutorily prescribed thirty-day period, Plaintiff will amend this Complaint to seek monetary damages against Defendants under Cal. Civ. Code §§ 1781 and 1782.

125. Plaintiff further seeks an order awarding costs of court and attorneys' fees under Cal. Civ. Code § 1780(e).

Prayer for Relief

WHEREFORE, Plaintiff Richard Spicer, on behalf of himself and the Class, seeks the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing Girard Gibbs LLP as Class Counsel, and finding that Plaintiff is a proper representative of the Class;

B. Declaratory relief, declaring Defendants' actions unlawful;

C. Injunctive relief, including an order prohibiting Defendants from peddling TrustedID's services on the breach notification website, and requiring Equifax to implement and maintain technical and administrative security controls that are appropriate for the type and amount of data it maintains.

D. Under causes of action other than the CLRA, damages, punitive damages (where appropriate), restitution, attorneys' fees, statutory costs, and such other and further relief as is just and proper.

Demand for Jury Trial

Plaintiff demands a trial by jury for all issues so triable.

Dated: September 8, 2017

Respectfully submitted,

GIRARD GIBBS LLP

By: */s/ Eric H. Gibbs*

Eric H. Gibbs (SBN 178658)

Amy Zeman (SBN 273100)
David M. Berger (SBN 277526
Adam E. Polk (SBN 273000)
Aaron Blumenthal (SBN 310605)
505 14th Street, Suite 1110
Oakland, CA 94612
Telephone: 510-350-9700
Facsimile: 510-350-9701
ehg@classlawgroup.com
amz@classlawgroup.com
dmb@classlawgroup.com
aep@girardgibbs.com
ab@classlawgroup.com

Attorneys for Plaintiff